No Direction Home: The True Cost of Routing Around Decoys

Amir Houmansadr

Edmund L. Wong

Vitaly Shmatikov

The University of Texas at Austin

Internet censorship

- The Internet is a big threat to repressive regimes!
- Repressive regimes censor the Internet:
  - IP filtering, DNS hijacking, deep packet inspection, …
- Circumvention systems

Tor

Anonymizer

The Freenet Project
http://freenetproject.org/

psiphon

Ultrasurf
PRIVACY. SECURITY. FREEDOM.

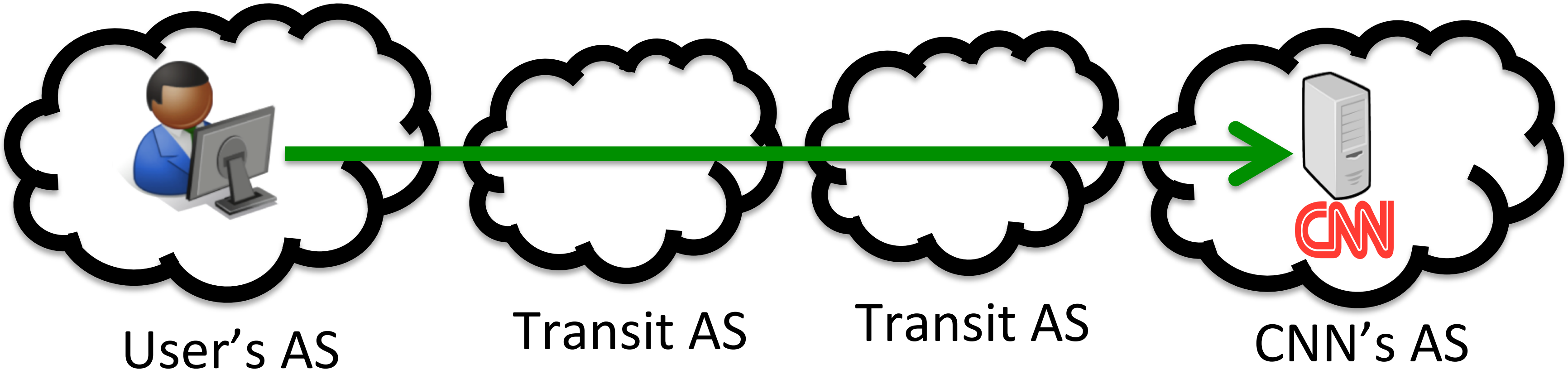
GPASS

Decoy routing circumvention

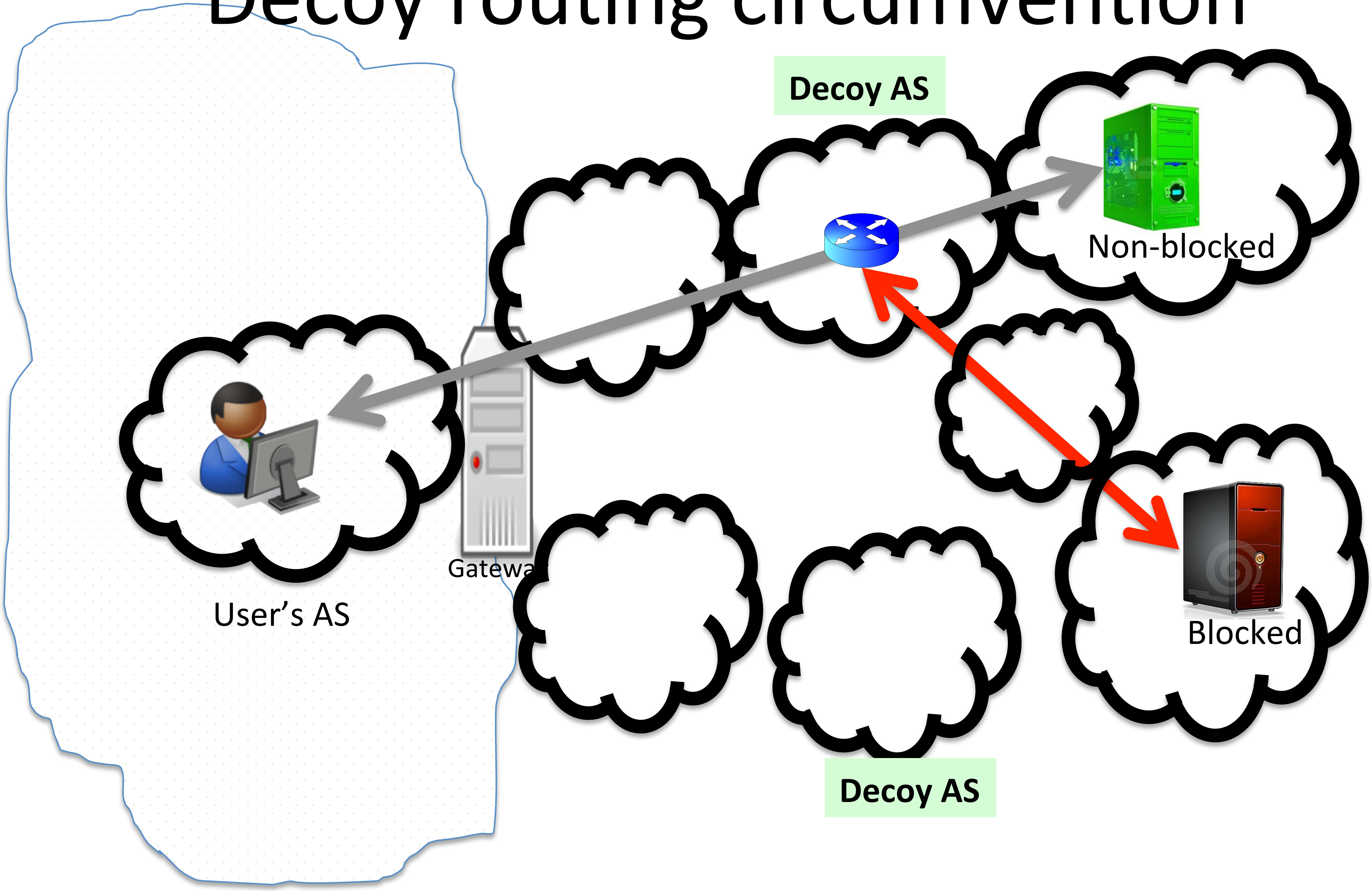
- DR (Karlin et al., FOCI 2011)
- Cirripede (Houmansadr et al., ACM CCS 2011)
- Telex (Wustrow et al., USENIX Security 2011)

Internet topology 101

- The Internet is composed of Autonomous Systems (ASes)
  - 44,000 ASes are inter-connected based on their business relationships



Decoy routing circumvention



Decoy AS

Non-blocked

User's AS

Gatewa

Blocked

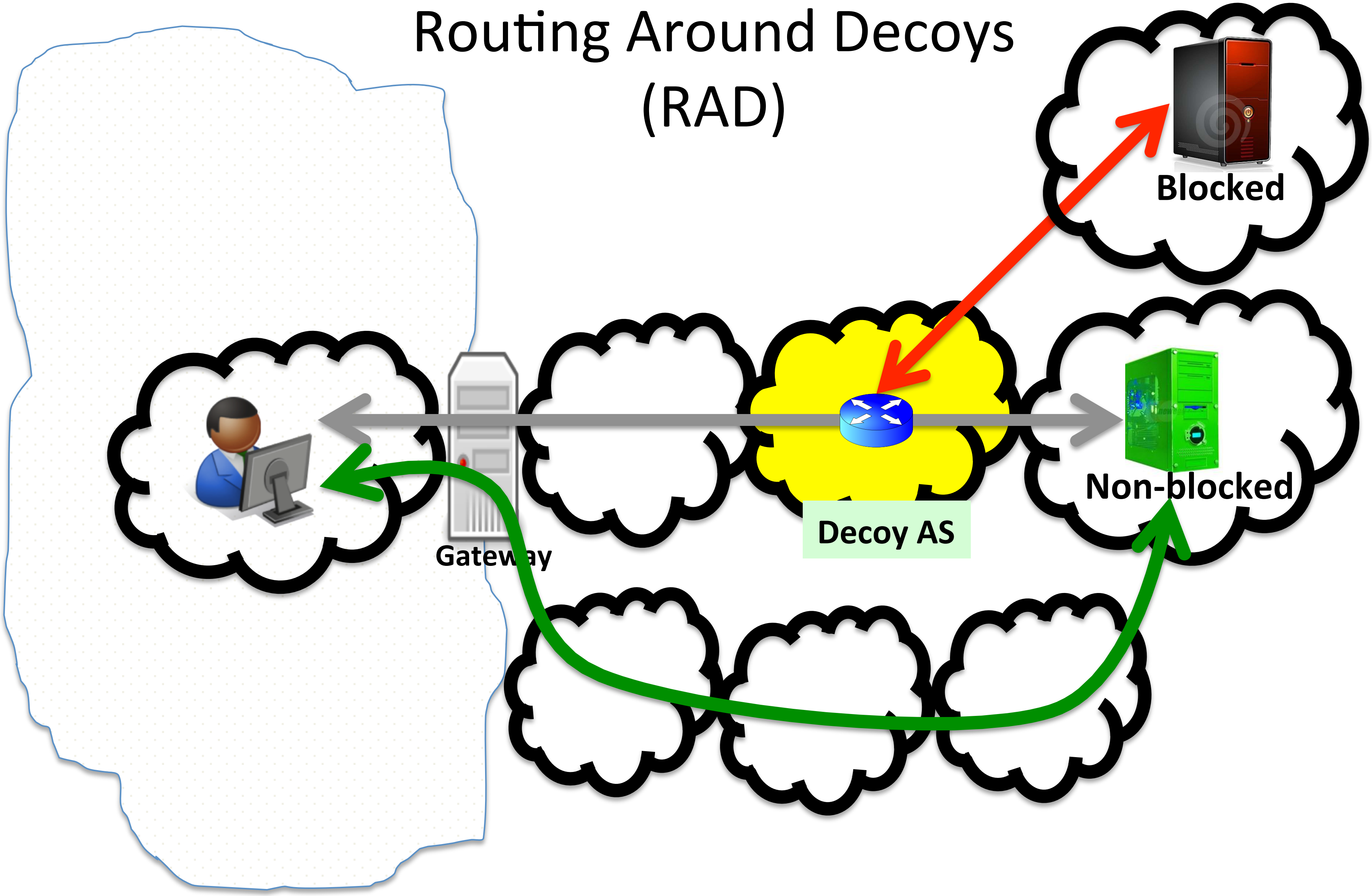
Decoy AS

The Non-Democratic Republic of Repressistan

Routing Around Decoys

Schuchard et al., ACM CCS 2012

Routing Around Decoys (RAD)



The Non-Democratic Republic of Repressistan

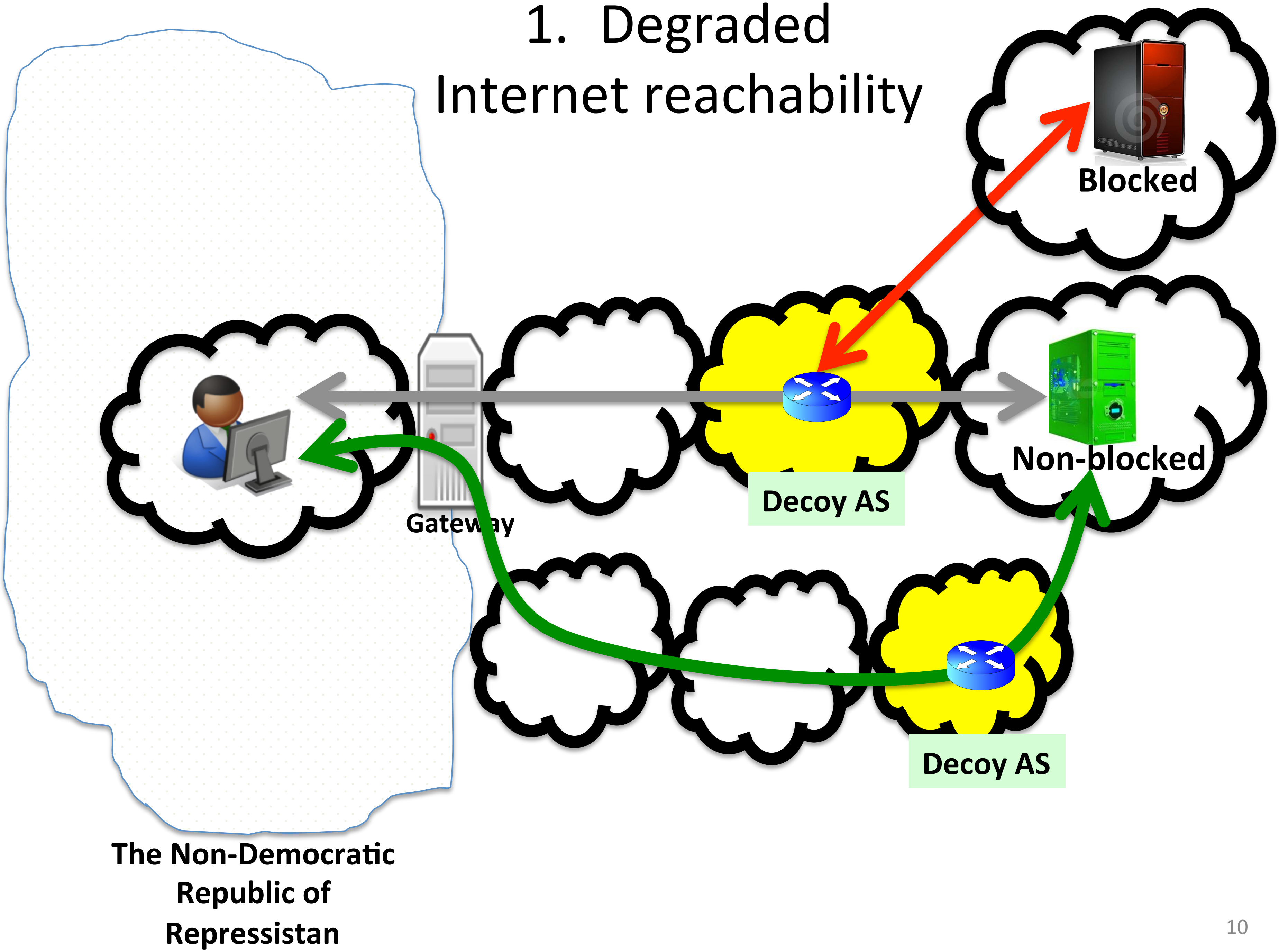
This paper

- Concrete analysis based on real inter-domain routing data
  - As opposed to relying on the AS graph only

- While technically feasible, RAD imposes significant costs to censors

- Main intuition: Internet paths are not equal!
  - Standard decision making in BGP aims to maximize QoS and minimize costs

1. Degraded Internet reachability



Path preference in BGP

- ASes are inter-connected based on business relationships
  - Customer-to-provider
  - Peer-to-peer
  - Sibling-to-sibling
- Standard path preference:
  1. Customer
  2. Peer/Sibling
  3. Provider

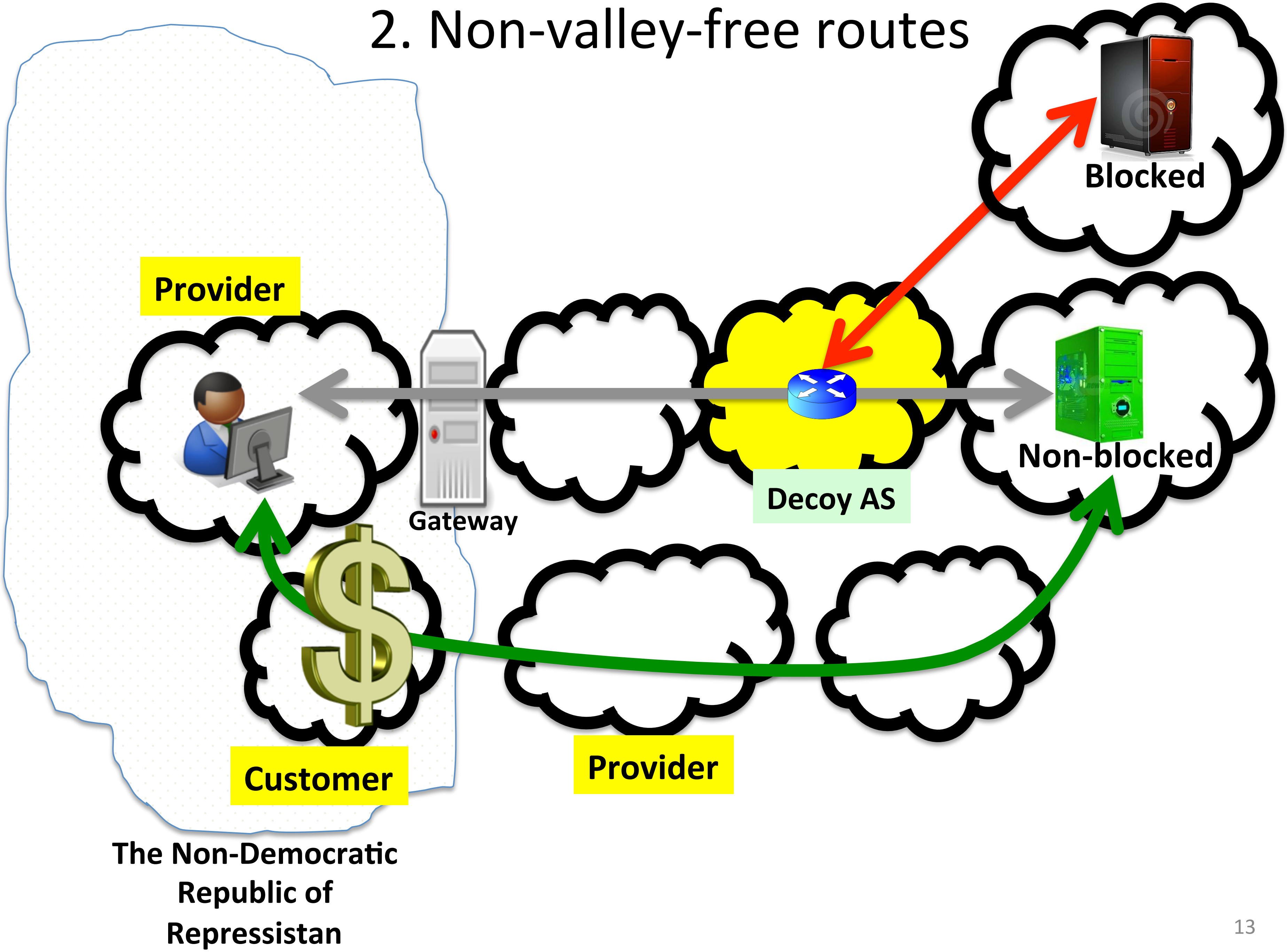
Valley-free routing

- A valley-free Internet path:

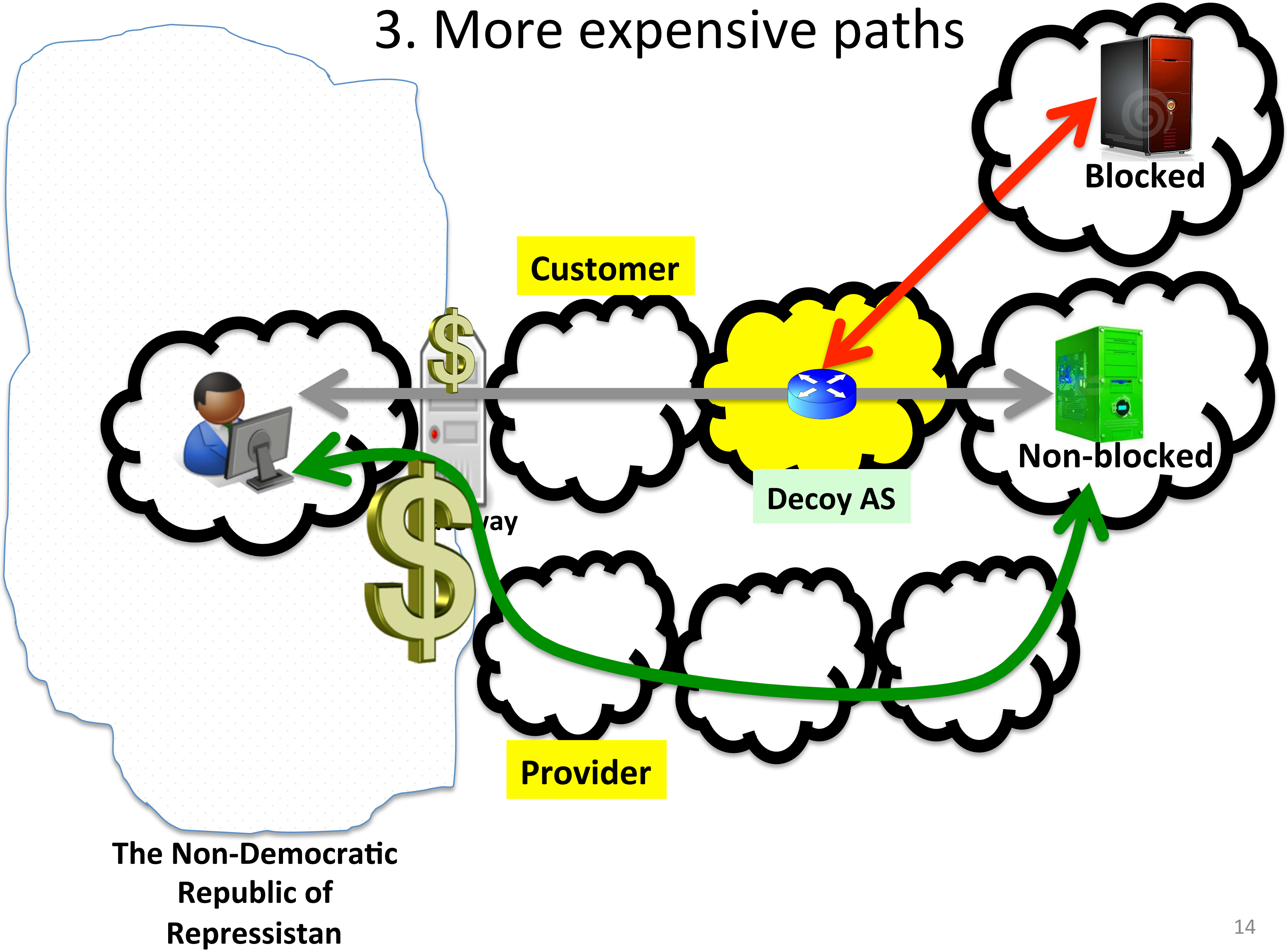
each transit AS is paid by at least one neighbor AS in the path

- ISPs widely practice valley-free routing

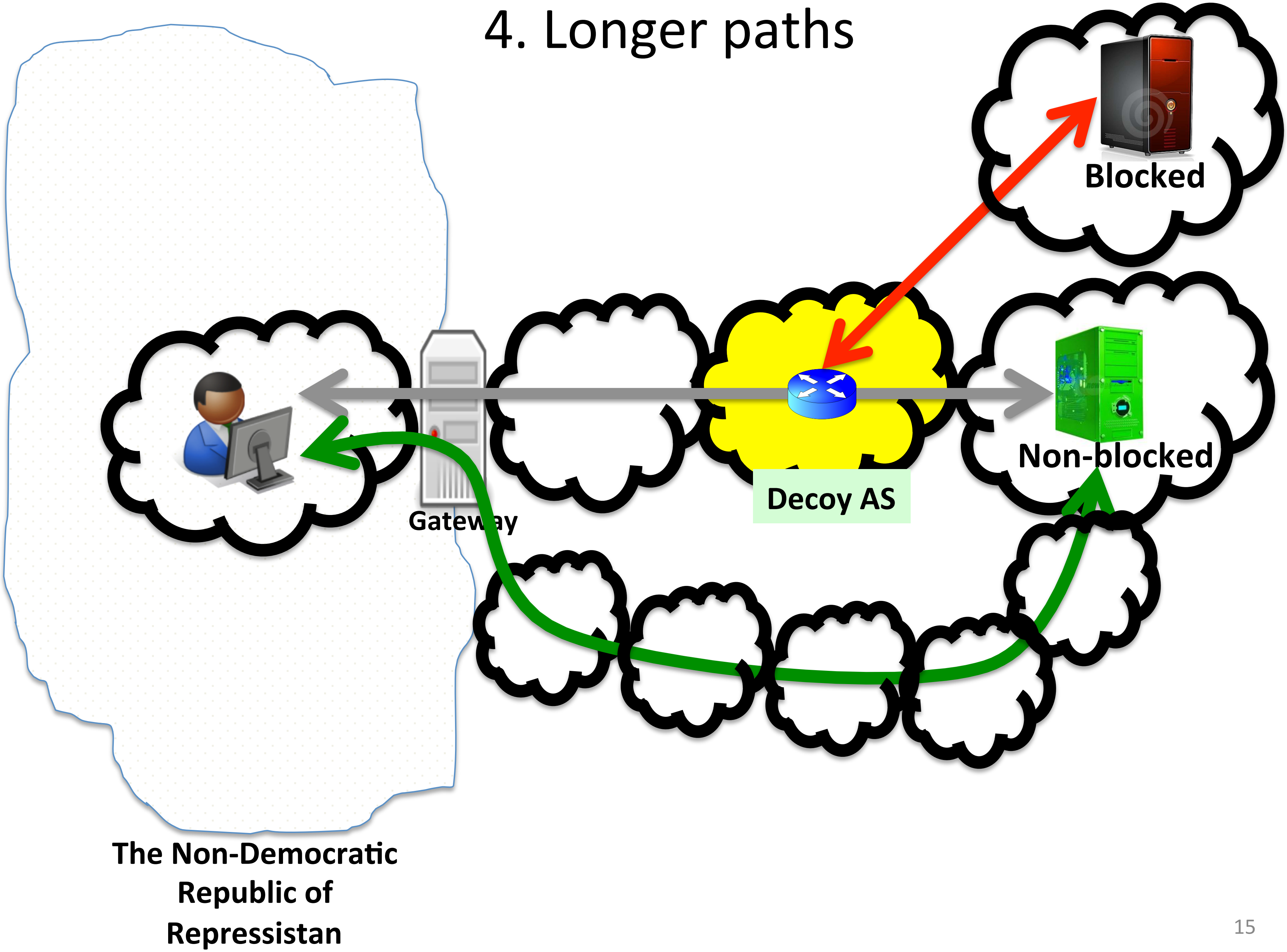
2. Non-valley-free routes



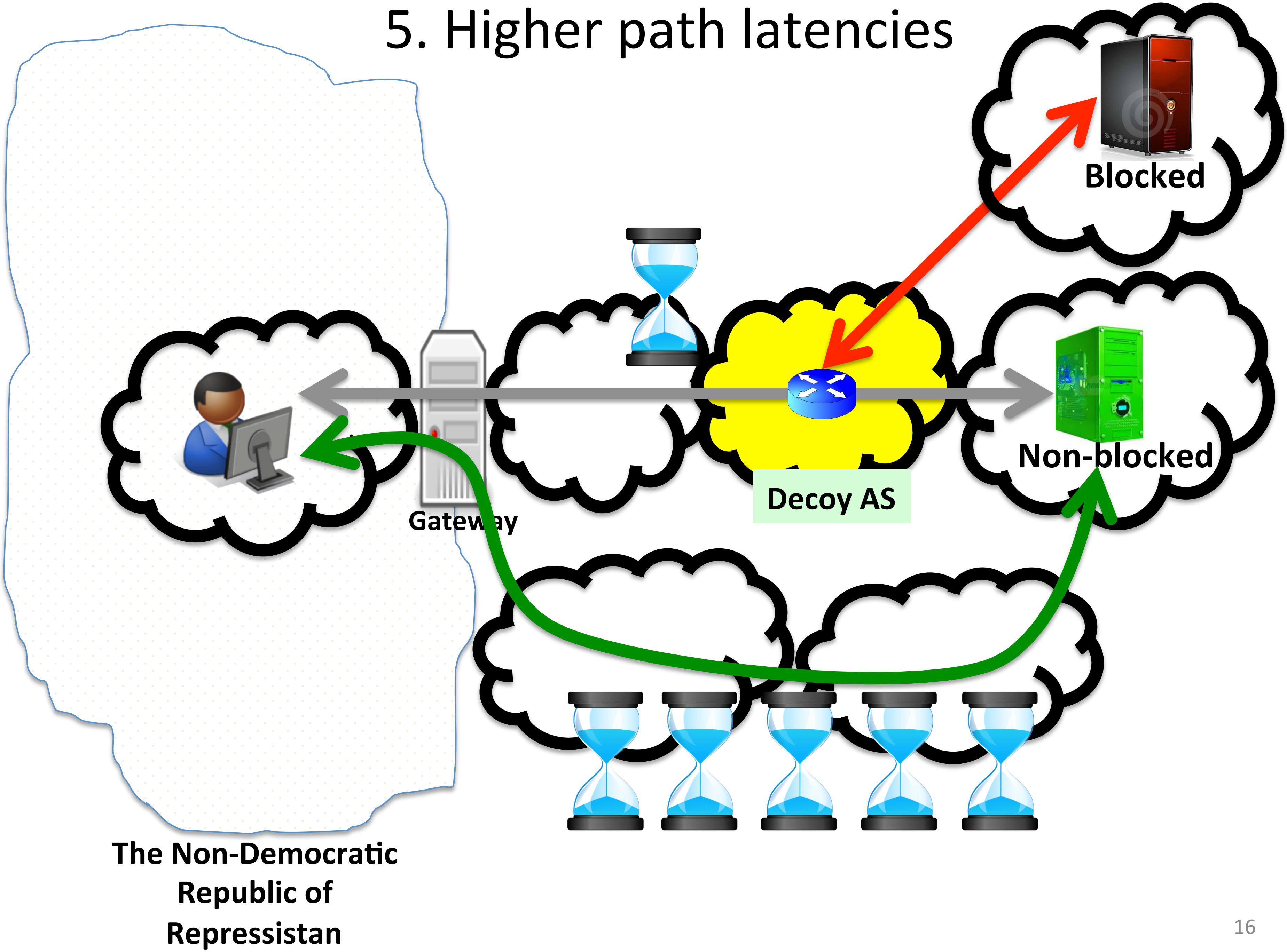
3. More expensive paths



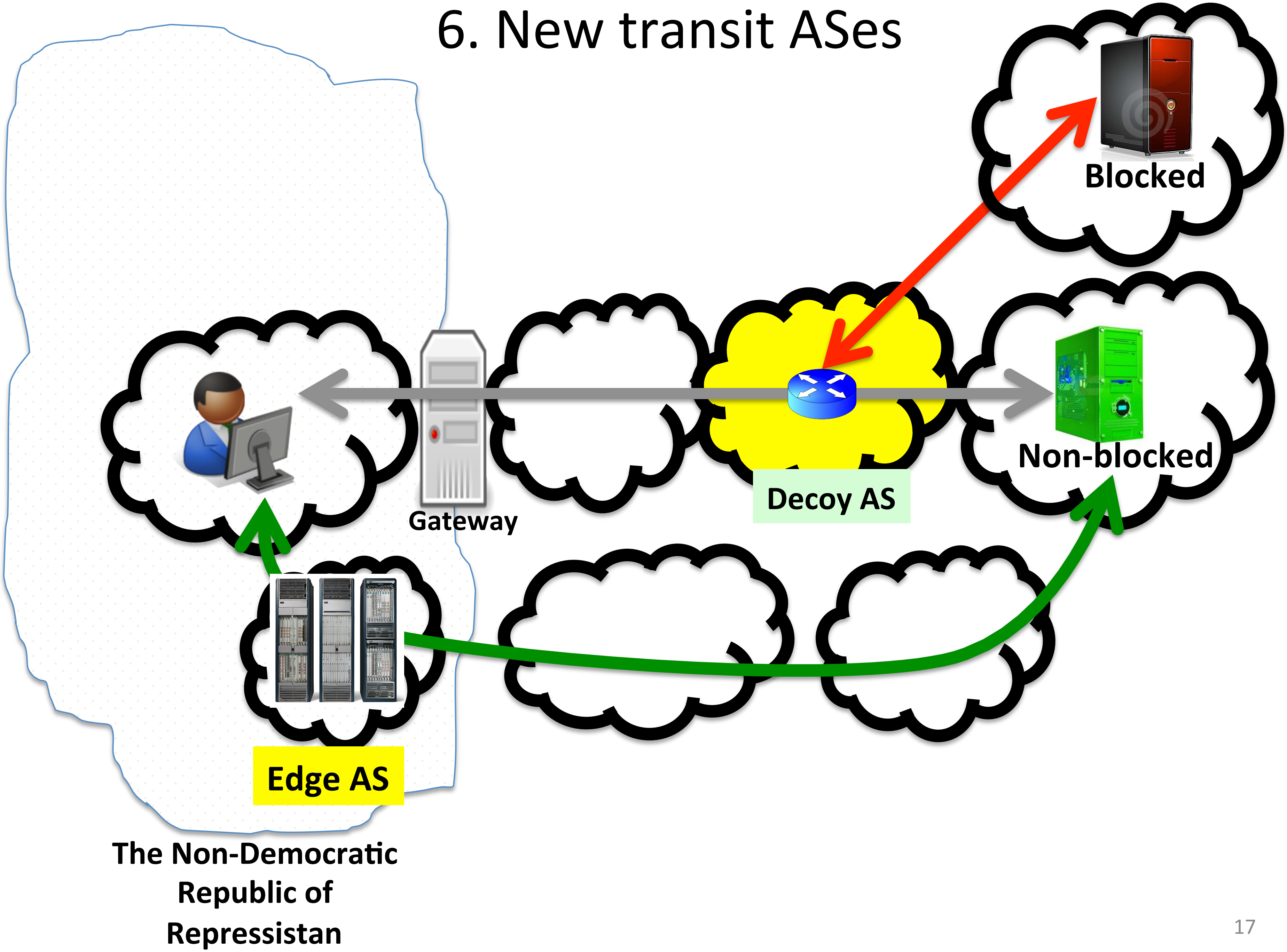
4. Longer paths



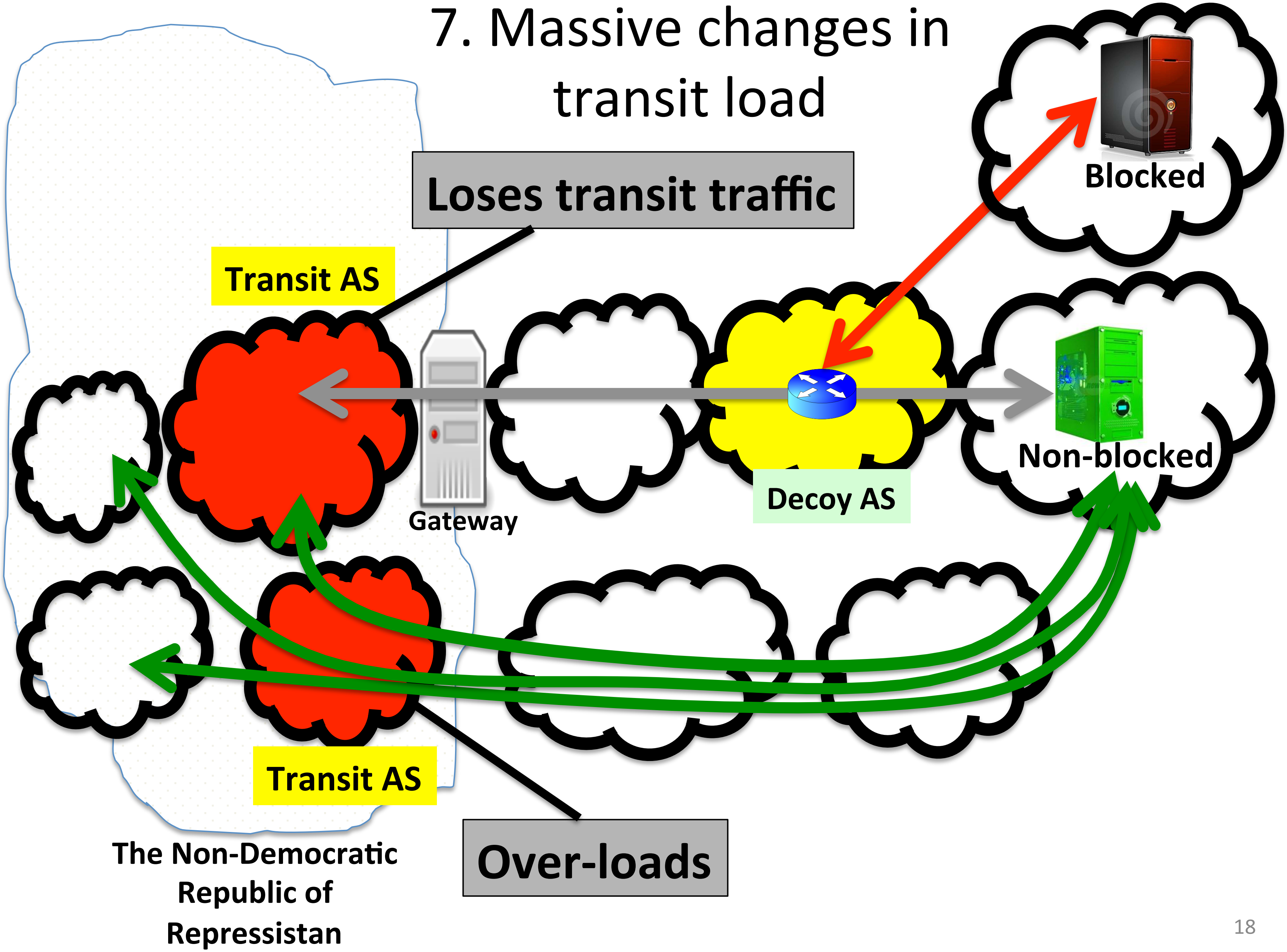
5. Higher path latencies



6. New transit ASes



7. Massive changes in transit load



Loses transit traffic

Transit AS

Blocked

Gateway

Decoy AS

Non-blocked

Transit AS

Over-loads

The Non-Democratic Republic of Repressistan

Simulations

- Use CBGP simulator for BGP
  - Python wrapper
- Datasets:
  - Geographic location (GeoLite dataset)
  - AS relations (CAIDA's inferred AS relations)
  - AS ranking (CAIDA's AS rank dataset)
  - Latency (iPlane's Inter-PoP links dataset)
  - Network origin (iPlane's Origin AS mapping dataset)
- Analyze RAD for
  - Various placement strategies
  - Various placement percentages
  - Various target/deploying Internet regions

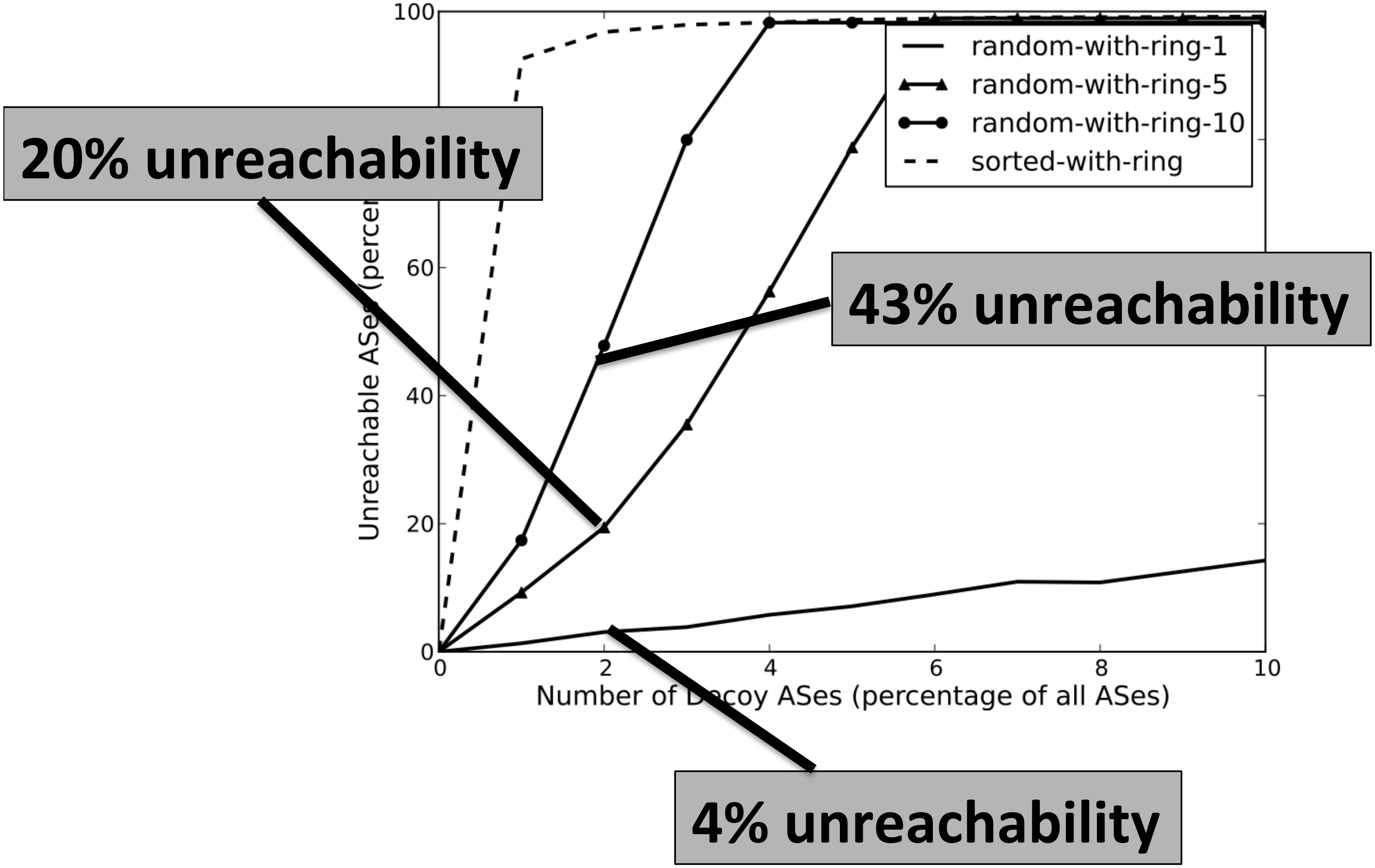
Costs for the Great Firewall of China

- A 2% random decoy placement disconnects China from 4% of the Internet
- Additionally:
  - 16% of routes become more expensive
  - 39% of Internet routes become longer
  - Latency increases by a factor of 8
  - The number of transit ASes increases by 150%
  - Transit loads change drastically (one AS increases by a factor of 2800, the other decreases by 32%)

Strategic placement

- RAD considers random selection for decoy ASes
  - This mostly selects edge ASes
  - Decoys should be deployed in transit ASes instead

Strategic placement



20% unreachability

43% unreachability

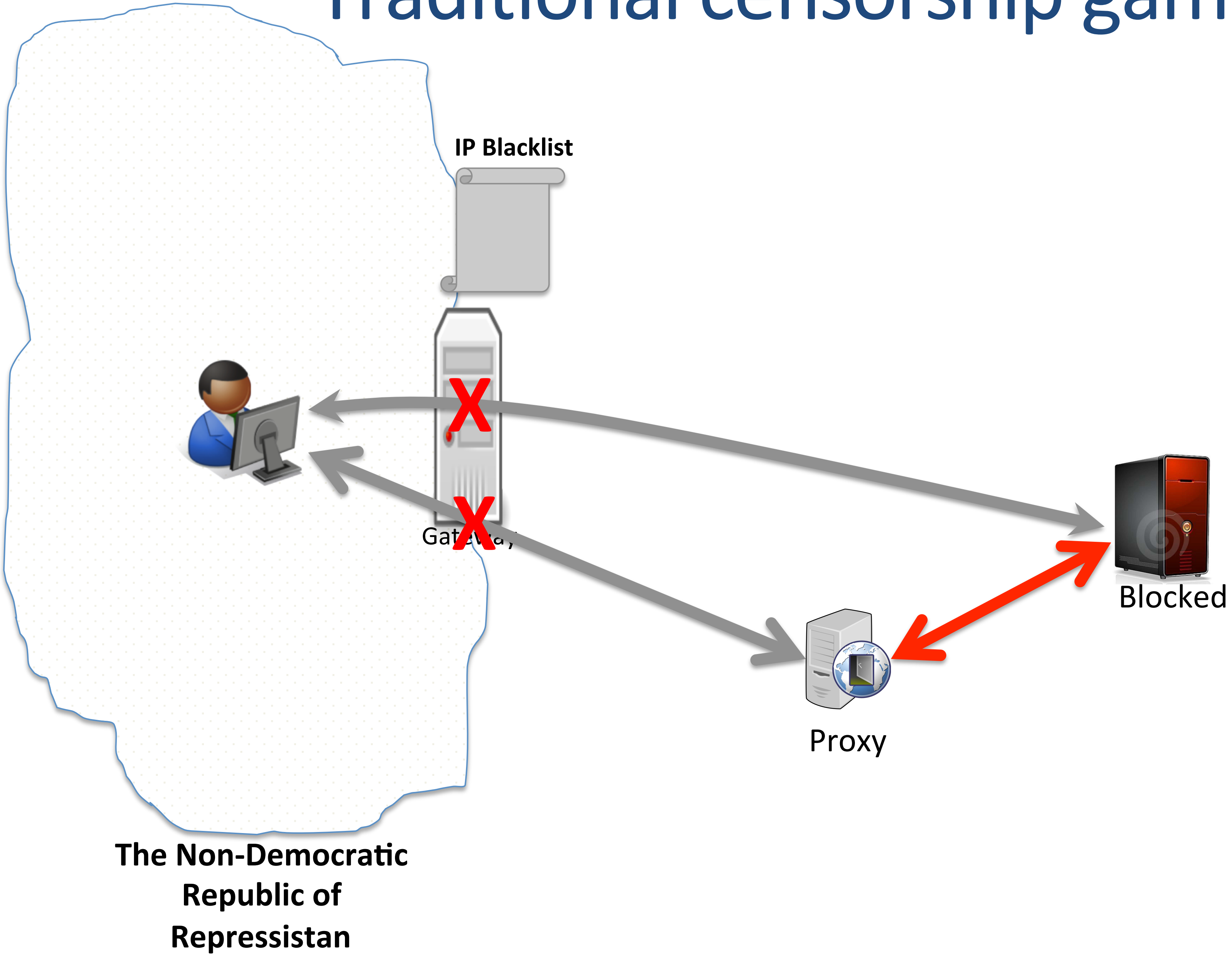
4% unreachability

Lessons

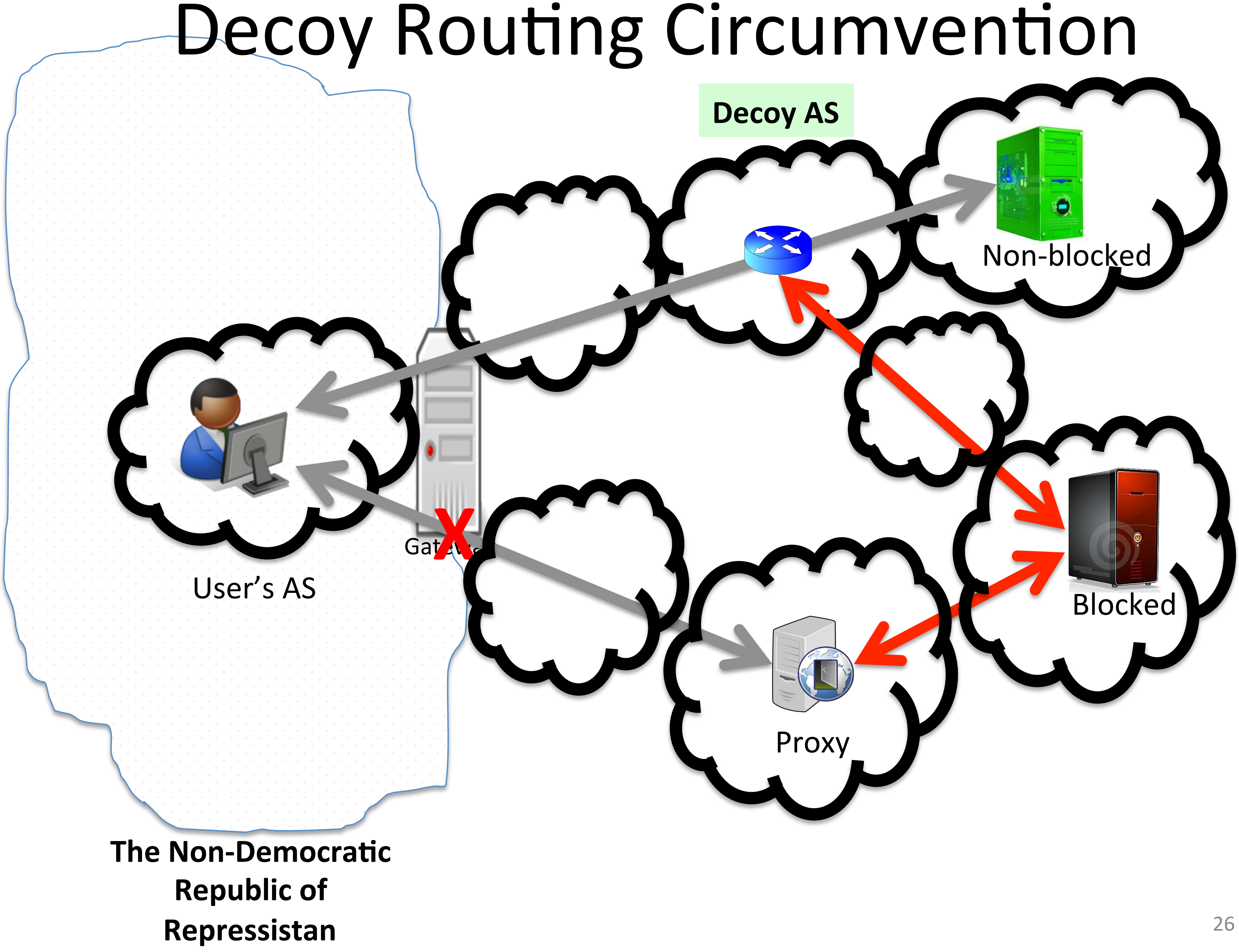
1. RAD is prohibitively costly to the censors
   - Monetary costs, as well as collateral damage
2. Strategic placement of decoys significantly increases the costs to the censors
3. The RAD attack is more costly to less-connected state-level censors
4. Even a regional placement is effective
5. Analysis of inter-domain routing requires a fine-grained data-driven approach

Thanks!

Traditional censorship game

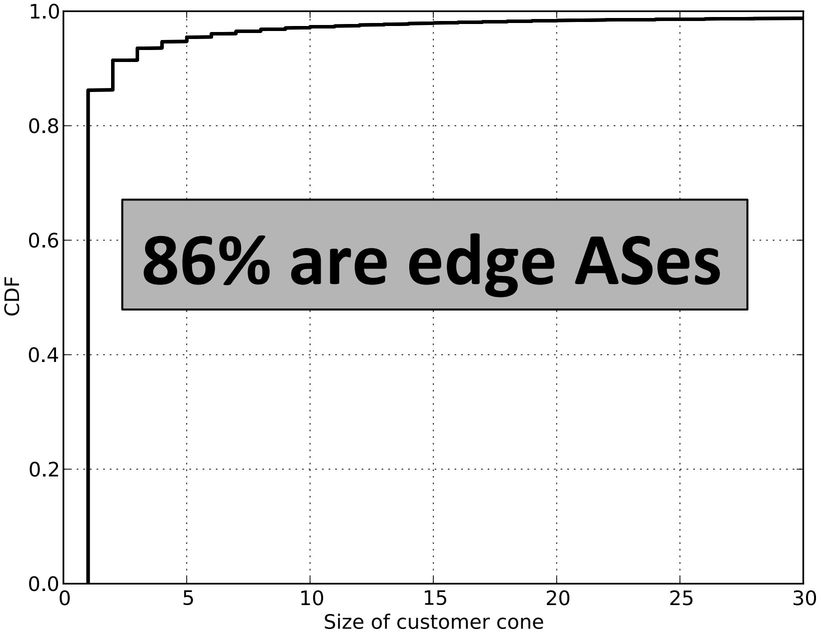


Decoy Routing Circumvention



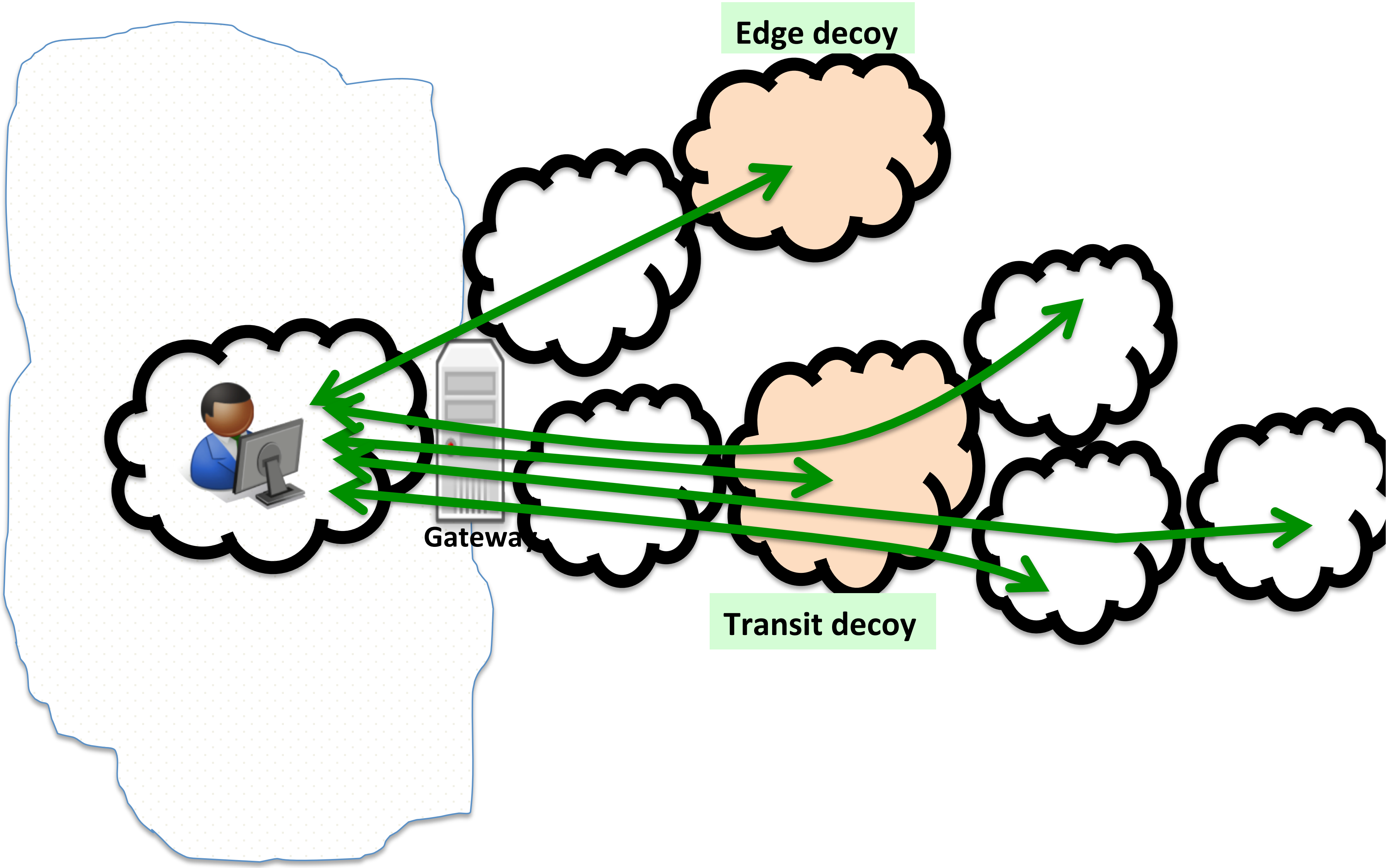
Strategic placement

- RAD considers random selection for decoy ASes



86% are edge ASes

- This mostly selects edge ASes



Edge decoy

Gateway

Transit decoy

The Non-Democratic Republic of Repressistan

Strategic placement

- Placements
  - *sorted*
  - *random-C*

- Amplifies the costs to a RAD censor
  - For a 2% deployment China is disconnected from 30% of all ASes, not 4%